UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/488,653	01/20/2000	Jun Tanaka	JA998-227	4753

7590 12/31/2003

Anne Vachon Dougherty
3173 Cedar Road
Yorktown Heights, NY 10598

EXAMINER	
TRIEU, LAURENT L	
ART UNIT	**PAPER NUMBER**
2137	3

DATE MAILED: 12/31/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/488,653	TANAKA ET AL.	
	Examiner	Art Unit	
	Laurent Trieu	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 January 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

1. Claims 1-27 are pending.

Claim Objections

2. Claim 9(b) is objected to because of the following informalities: "Causing" is misspelled as "causnig". Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-27 are rejected under 35 U.S.C. 102(b) as being anticipated by Isikoff, US Patent Number 5,748,084.

Regarding claims 1 –

1(a) "storing data" is met by "firmware or other logic" (column 4, line 48)

1(c) "using said data stored" is met by "the security logic identifies an alarm condition" (Column 4, lines 5-6)

1(d) "detecting" is met by "beacon determines that the antenna has been destroyed or tampered with" (Column 4, lines 58-60)

1(b) "starting a procedure" and 1(e) "prohibiting access" is met by "actuates its various internal security protocols" (Column 4, line 60)

Regarding claim 2 –

Isikoff discloses, "an improper attempt to start the computer..." (Column 9, lines 13-14). This reads on "wherein said step (b) is initiated in response to a trigger event."

Regarding claim 3 –

Isikoff discloses, "for instance, when they detect unusual activity such as a failed password entry" (Column 9, lines 10-11). This reads on "wherein said step (e) is performed only when an authorized password is not entered".

Regarding Claims 5 - 7

5(a) & 7(a) "storing data" is met by "firmware or other logic" (column 4, line 48)

5(c) & 7(c) "using said data stored" is met by "the security logic identifies an alarm condition" (Column 4, lines 5-6)

5(d) & 7(d) "detecting" is met by "beacon determines that the antenna has been destroyed or tampered with" (Column 4, lines 58-60)

5(b) & 7(b)"starting a procedure" and 5(e) & 7(e)"prohibiting access" is met by "actuates its various internal security protocols" (Column 4, line 60)

Claim 6's "a central processing unit periodically monitoring the security device" and claim 7's "central processing unit" are met by "a microprocessor" (Column 3, line 65) and Fig. 3, item 30 and "sensors are provided that detect various physical parameters" (Column 8, line 65- Column 9, line 4). "Periodically" is read on by "attempt to start the computer..." (Column 9, lines 13-14). Furthermore claim 7's "storing data while a main power source of said computer is turned off" is met by "The beacon may also contain its own back-up battery to enhance the ability of the beacon to operate when power to the main computer is removed or run down" (Column 9, lines 15-17)

Regarding claims 4 & 8 –

Claims 4(e) and 8 (e) "storing data indicating..." are read on by "low level security codes." (Column 6, line 16)

Regarding claim 9 –

- "first storage means capable of storing data while a main power source of said computer is turned off" is read on by "The beacon may also contain its own back-up battery to enhance the ability of the beacon to operate when power to the main computer is removed or run down" (Column 9, lines 15-17)
- "a central processing unit" is read on by "the security logic" (Column 9, line 5)
- "(a) storing data indicating that said security device was attached to said computer in a first region of the first storage means in said computer; (b) causing the central processing unit in said computer to periodically monitor to determine whether said security device has been removed from said computer; and (c) prohibiting access to

said computer in response to a determination in step (b) that the security device has been removed" are read on by "When these sensors detect unusual activity such as removal or physical tampering with a lock, switch, board or antenna, the security logic identifies an alarm condition and actuates the beacon so it performs such actions as erasing the hard drive, calling for help, transmitting important files or the like." (Column 9, lines 4-9). The steps of "storing" and "monitoring" are inherent in the "detection" step of "unusual activity". Without storing such information, the machine/apparatus would not be able to differentiate between "usual" and "unusual activity".

Regarding claim 10 –

- "first storage means capable of storing data while a main power source of said computer is turned off" is read on by "The beacon may also contain its own back-up battery to enhance the ability of the beacon to operate when power to the main computer is removed or run down" (Column 9, lines 15-17)
- "a central processing unit" is read on by "the security logic" (Column 9, line 5)
- means for storing data indicating that said security device was attached to said computer in a first region of the first storage means; first detection means for using said data stored in said first region to detect that said security device was once attached to said computer; second detection means for detecting that said security device has been removed from said computer; and means for prohibiting access to said computer in response to said detection means" are read on by "When these

sensors detect unusual activity such as removal or physical tampering with a lock, switch, board or antenna, the security logic identifies an alarm condition and actuates the beacon so it performs such actions as erasing the hard drive, calling for help, transmitting important files or the like." (Column 9, lines 4-9). The steps of "storing" and "monitoring" are inherent in the "detection" step of "unusual activity". Without storing such information, the machine/apparatus would not be able to differentiate between "usual" and "unusual activity".

Regarding claim 11 –

- means for storing, in response to said first and said second detection means data indicating that said security device that was once attached to said computer has been removed therefrom in a second region of said first storage means; and means for prohibiting, in response to said data stored in said second region, access to said computer" are read on by "When these sensors detect unusual activity such as removal or physical tampering with a lock, switch, board or antenna, the security logic identifies an alarm condition and actuates the beacon so it performs such actions as erasing the hard drive, calling for help, transmitting important files or the like." (Column 9, lines 4-9). The steps of "storing" and "monitoring" are inherent in the "detection" step of "unusual activity". Without storing such information, the machine/apparatus would not be able to differentiate between "usual" and "unusual activity".

Regarding claim 12 –

- "first storage means capable of storing data while a main power source of said computer is turned off" is read on by "The beacon may also contain its own back-up battery to enhance the ability of the beacon to operate when power to the main computer is removed or run down" (Column 9, lines 15-17)
- "a central processing unit" is read on by "the security logic" (Column 9, line 5)
- means for storing data indicating that said security device that was once attached to said computer has been removed therefrom in a region of the first storage means; detection means for using said data stored in said region to detect that said security device attached to said computer has been removed therefrom; and means for prohibiting, in response to said detection means, access to said computer." are read on by "When these sensors detect unusual activity such as removal or physical tampering with a lock, switch, board or antenna, the security logic identifies an alarm condition and actuates the beacon so it performs such actions as erasing the hard drive, calling for help, transmitting important files or the like." (Column 9, lines 4-9). The steps of "storing" and "monitoring" are inherent in the "detection" step of "unusual activity". Without storing such information, the machine/apparatus would not be able to differentiate between "usual" and "unusual activity".

Regarding claim 13 –

"first storage means capable of storing data while a main power source of said computer is turned off" is read on by "The beacon may also contain its own back-up

battery to enhance the ability of the beacon to operate when power to the main computer is removed or run down" (Column 9, lines 15-17)

- "means for storing data indicating that said security device was attached to said computer in a region of the first storage means; a central processing unit for monitoring periodically to determine whether said security device has been removed from said computer; and means for prohibiting access to said computer in response to a result obtained by said central processing unit." are read on by "When these sensors detect unusual activity such as removal or physical tampering with a lock, switch, board or antenna, the security logic identifies an alarm condition and actuates the beacon so it performs such actions as erasing the hard drive, calling for help, transmitting important files or the like." (Column 9, lines 4-9). The steps of "storing" and "monitoring" are inherent in the "detection" step of "unusual activity". Without storing such information, the machine/apparatus would not be able to differentiate between "usual" and "unusual activity".

Regarding claims 14-20 –

- "wherein said first storage means is an RFID tag 'used by an RFID system, and said security device is an RF antenna" is read on by "an RF pager-based system" (Column 9, line 4) where pager is read to comprise an RFID tag.

Regarding claims 21-27 –

- "wherein said RF antenna is attached to a lid of a device bay of said computer" is rejected by figure 5 which discloses the antenna being attached to the computer lid. Isikoff also discloses, "as shown in FIG. 5, the antenna 60 for the beacon 101 is incorporated into the design for the computer allowing many possibilities for different antenna configurations." (Column 4, lines 23-26).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Laurent Trieu whose telephone number is 703-305-0712. The examiner can normally be reached on Monday - Friday, 7AM - 4PM ET.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100